IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRIT OF GEORGIA
ATLANTA DIVISION

BRITTANY FELIX, individually and on behalf of all similarly situated persons, Plaintiff, v. HOSPITALITY STAFFING SOLUTIONS, LLC, Defendant.	**Civil Action No.:** PROPOSED CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Brittany Felix ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to her and on information and belief as to all other matters, by and through counsel, hereby brings this Class Action Complaint against Defendant, Hospitality Staffing Solutions, LLC ("HSS" or "Defendant").

NATURE OF THE ACTION

1. In June 2023, HSS, a company that partners with hospitality leaders across the country and assists with employment opportunities for individuals looking for work in the hospitality industry, lost control over its employees' and customers' highly sensitive personal information in a data breach by cybercriminals ("Data Breach").

2. The Data Breach compromised the "personally identifiable information" ("PII") belonging to employees and customers, including their Social Security numbers, driver's license numbers, and financial account numbers. As a result, Plaintiff and proposed Class Members no longer have control over their most sensitive information, cannot stop others from viewing it, and cannot prevent criminals from misusing it.

3. What's more, the Data Breach exposed Plaintiff and Class Members to an increased lifelong risk for identity theft and fraud. Indeed, the Data Breach included information individuals cannot change, like their Social Security numbers.

4. Upon information and belief, the PII of Plaintiff and Class Members has already been misused. This is not a case where an unidentified third party may have possibly viewed PII. Here, the cybercriminals who gained access to HSS's network are identified and have a voice – they stole the information and have advertised posting it for sale on the dark web.

5. Indeed, as described herein, Akira, a ransomware group, advertised on June 29, 2023, that it was uploading 1.3 terabytes of data containing detailed employee and customer information, would be uploaded to its dark web blog and made readily for even more criminals to access.

6. HSS exacerbated the harm Plaintiff and Class Members are suffering by failing to adequately and transparently notify them about the Data Breach,

including failing to notify them that Akira was posting their PII on the dark web.

7. HSS's Data Breach should not have happened because it was preventable.

8. HSS knows it has duties to safeguard private information.

9. Employees and customers, like Plaintiff, relied on HSS to fulfill its duties when they agreed to use HSS's services, and they would not have used HSS's services if HSS had not promised to protect their PII ("Personal Information").

10. On information and belief, HSS failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over the access to Personal Information. HSS's negligence is evidenced by its failure to prevent, detect, or stop the Data Breach before criminals gained access to HSS's systems and stole the information belonging to Plaintiff and Class Members.

11. HSS's misconduct violates state and federal law and industry standard data security policies.

PARTIES

12. Plaintiff Brittany Felix is a resident and citizen of South Carolina.

13. Defendant Hospitality Staffing Solutions, LLC is an LLC with its corporate office located at 1117 Perimeter Center West, Suite E401, Atlanta, Georgia 30338.

14. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known, including the members of the LLC.

JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C.§ 1332 (d). The amount in controversy exceeds $5,000,000 exclusive of interest and costs, there are more than one hundred putative class members, and at least one putative class member is a citizen of a different state than Defendant.

16. This Court has personal jurisdiction over HSS because HSS maintains its principal place of business in this District and is authorized to and does conduct substantial business in this District.

17. Venue is proper in this Court because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in, was directed to, and/or emanated from this District, HSS is based in this District, HSS maintains Personal Information in this District, and has caused harm to Class Members residing in this District.

FACTUAL BACKGROUND

A. HSS Collects and Promises to Protect Personal Information

18. HSS is the largest national staffing company specializing in hospitality. HSS claims to provide the most highly regarded properties with a superior, reliable, motivated workforce and is the "standard setting staffing and services provider of choice" to a demanding and changing industry.[1]

19. HSS's more than 12,000 employees serve in hotels, resorts, and casinos across the country.

20. To operate its business, HSS must collect and store Personal Information from individuals it hires and conducts business with.

21. As a result, HSS requires individuals to disclose their Personal Information to receive HSS's services, including their Social Security numbers, drivers' license numbers, and financial information.

22. In so doing, HSS promises those individuals it will protect their information under state and federal law and its internal policies.

23. In fact, HSS assures Plaintiff and Class Members that "confidence and trust are important to [HSS]." In other words, HSS recognizes it has duties to safeguard Personal Information. *See* HSS's Data Breach Notice ("Notice," attached as **Exhibit A**).

[1] *See*, https://www.hssstaffing.com/history/ (last visited Aug. 4, 2023).

24. Upon information and belief, HSS never implemented the security safeguards necessary to fulfill those duties, failing to adequately train its employees on data security, develop policies to prevent breaches, enforce those policies, follow industry standard guidelines on cybersecurity, and timely respond to data breaches and inform affected individuals as required by law.

25. As a result, HSS left Plaintiff and Class Members' Personal Information an unguarded target for theft and misuse.

B. HSS Violates Its Duties to Plaintiff and Class Members

26. In June 2023, HSS discovered that an unauthorized third party accessed HSS's network environment.

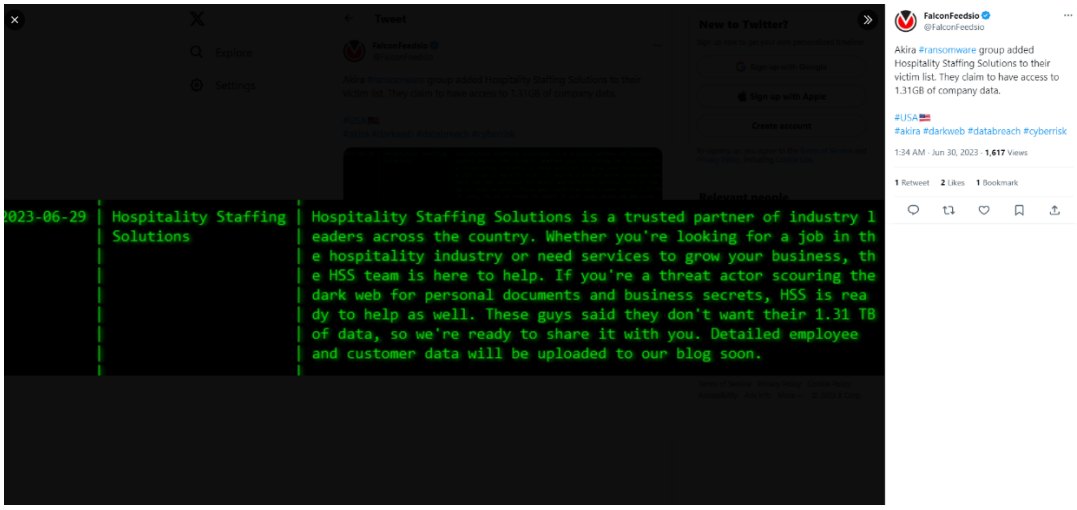
27. In other words, HSS experienced a data breach by cybercriminals, who bypassed HSS's lax security and infiltrated its systems.

28. Once inside, hackers could access Plaintiff and Class Members' Personal Information, including their Social Security numbers, drivers' license numbers, and financial information.

29. On information and belief, the Data Breach was a "ransomware" attack, meaning criminals blocked HSS's access to data and held it ransom. This fact was not disclosed by HSS in the Notice it provided Plaintiff and Class Members.

30. On information and belief, Akira, a known-ransomware group, took responsibility for the ransomware attack on June 29, 2023. Falcon Feeds, a

technology-security company and threat intelligence platform for cyber security professionals, alerted the public to the following dark web announcement from Akira on June 30, 2023, via Twitter[2]:



31. According to Akira, in response to the ransomware attack, HSS indicated that it did not "want their 1.21 TB of data, so [Akira is] ready to share it with [cybercriminals]. Detailed employee and customer data will be uploaded to our blog soon."

32. Akira's statements contradict those made by HSS in its Notice to Plaintiff and Class Member, where it claims that upon discovery of the infiltration on June 2, 2023, HSS "immediately took steps to secure [its] systems."

33. HSS did not warn Plaintiff and Class Members that it permanently lost control over their data and that their Personal Information has been posted to the

[2] *See also*, https://twitter.com/FalconFeedsio/status/1674652638590238722 (last accessed Aug. 7, 2023).

dark web by cybercriminals, meaning they have no reason to guard themselves against identity theft and fraud. This deception means individuals will continue to work with HSS, providing their Personal Information to an unsecure company and HSS continuing to collect revenue associated with its business.

34. In its Notice, HSS vaguely encouraged Plaintiff and Class Members to "remain vigilant" by reviewing account statements and credit reports for unauthorized activity.

35. In other words, HSS encouraged Plaintiff and Class Members to spend time and resources mitigating the harm resulting from the Data Breach while providing no details as to the scope or severity.

36. HSS foresaw the harm that would result from the Data Breach; indeed as Plaintiff has suffered harm following HSS's Data Breach.

C. Plaintiff's Experience

37. Plaintiff Felix was employed with HSS through a temp agency. As a result, Plaintiff provided her Personal Information to HSS as a condition of employment.

38. Plaintiff is a victim of the Data Breach, having received HSS's Notice in August 2023.

39. Plaintiff provided her Personal Information, including her Social Security number and financial information, to HSS and trusted that HSS would use

reasonable measures to protect it. Plaintiff expected that information would be protected according to state and federal law and any applicable internal policies at the company—here, HSS.

40. Upon information and belief, cybercriminals not only viewed her Personal Information, but stole it and subsequently advertised it for sale on the dark web, causing actual and concrete harm to Plaintiff. Plaintiff's risk of identity theft and fraud is certain and imminent.

41. To deal with this substantially increased risk of fraud and identity theft, Plaintiff has devoted several hours attempting to mitigate the harm caused by the Data Breach.

42. Indeed, Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what Personal Information was exposed in the Data Breach.

43. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. The fear stems from the fact that her highly sensitive Personal Information is in criminal hands, who have already misused her information. These emotional harms go far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

44. Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

45. Plaintiff does not recall ever learning that her information was compromised in a data breach incident, other than the Data Breach at issue in this case.

46. Plaintiff has a continuing interest in ensuring that her Personal Information, which is the type that cannot be changed and upon information and belief remains in HSS's possession, is protected and safeguarded from future breaches.

47. HSS has not represented the business practices changes that have been implemented to prevent against further data breaches—even at a high level that would not jeopardize its security infrastructure.

D. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

48. Plaintiff and Class Members have suffered injury from the misuse of their Personal Information that can be directly traced to HSS.

49. As a result of HSS's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Personal

Information is used;

b. The compromise and continuing publication of their Personal Information;

c. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

d. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

e. Delay in receipt of tax refund monies;

f. Unauthorized use of stolen Personal Information; and

g. The continued increased risk to their Personal Information, which remains in the possession of HSS and is subject to further breaches so long as HSS fails to undertake the appropriate measures to protect the Personal Information in their possession.

50. Stolen Personal Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Personal Information can be worth up to $1,000.00 depending on the type of information obtained. Thus, criminals willingly pay money

for access to Personal Information, which enables those criminals to commit fraud and identity theft to the detriment of employees and consumers, including Plaintiff and members of the Class.

51. The value of Plaintiff's and the proposed Class's Personal Information on the black market is considerable. Stolen Personal Information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

52. It can take victims years to spot identity or Personal Information theft, giving criminals plenty of time to use that information for cash.

53. One such example of criminals using Personal Information for profit is the development of "Fullz" packages.

54. Cyber-criminals can cross-reference two sources of Personal Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

55. The development of "Fullz" packages means that stolen Personal Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails,

phone numbers, or credit card numbers may not be included in the Personal Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen Personal Information are being misused, and that such misuse is fairly traceable to the Data Breach.

56. HSS disclosed the Personal Information of Plaintiff and members of the proposed Class to unauthorized third parties to use in the conduct of criminal activity. Specifically, HSS exposed the Personal Information of the Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Personal Information.

57. HSS's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Personal Information and take other necessary steps to mitigate the harm caused by the Data Breach.

58. Had HSS properly notified Plaintiff and members of the proposed Class of the Data Breach, Plaintiff and members of the proposed Class could have taken proactive, rather than reactive, mitigating measures.

E. HSS failed to adhere to FTC guidelines.

59. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as HSS, should employ to protect against the unlawful exposure of Personal Information.

60. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

61. The guidelines also recommend that businesses watch for large

amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

62. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

63. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

64. HSS's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS REPRESENTATION ALLEGATIONS

65. Plaintiff brings this suit on behalf of herself and a class of similarly situated individuals under Federal Rule of Civil Procedure 23 on behalf of a class preliminarily defined as:

> All persons impacted by the Data Breach, including all who were sent a notice of the Data Breach.
>
> Excluded from the class are all employees, officers, and directors of Defendant, as well as any judges presiding over this matter and court personal assigned to this case.

66. **Numerosity**: The Class Members are so numerous that joinder of all members is impracticable. The exact number and identities of Class Members are unknown at this time, but believed to be, at least, in the thousands based on the 1.21 TB of data compromised. The identities of Class Members are ascertainable through HSS's records, Class Members' records, publication notice, self-identification, and other means.

67. **Commonality:** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the Class. Common questions include, but are not limited to, the following:

(a) Whether HSS violated state and federal laws by failing to properly store, secure, and dispose of Plaintiff's and Class Members' Personal Information;

(b) Whether HSS failed to employ reasonable and adequate data and cybersecurity measures in compliance with applicable state and federal regulations;

(c) Whether HSS acted willfully, recklessly, or negligently with regard to securing Plaintiff's and Class Members' Personal Information;

(d) How the Data Breach occurred;

(e) Whether HSS failed to adequately notify Plaintiff and Class Members of the Data Breach;

(f) Whether Plaintiff and Class Members are entitled to restitution, damages, compensation, or other monetary relief; and

(g) Whether Plaintiff and Class Members are entitled to injunctive and declaratory relief necessary to secure their Personal Information from further intrusion, exposure, and misuse.

68. Common sources of evidence may also be used to demonstrate HSS's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove HSS's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

69. **Typicality:** Plaintiff's claims are typical of the claims of the respective Class they seek to represent, in that the named Plaintiff and all members of the proposed Class have suffered similar injuries as a result of the same practices alleged herein. Plaintiff has no interests adverse to the interests of the other members of the Class.

70. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the Class and have retained attorneys well experienced in class actions and complex litigation as their counsel, including cases alleging consumer protection and data privacy claims arising from data breaches.

71. Plaintiff avers that the prosecution of separate actions by the individual members of the proposed Class would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for HSS; that the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; that HSS has acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed Class as a whole; that questions of law or fact common to the Class predominate over any questions affecting only individual members and

that class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy which is the subject of this action. Plaintiff further state that the interests of judicial economy will be served by concentrating litigation concerning these claims in this Court, and that the management of the Class will not be difficult.

72. Plaintiff and other members of the Class have suffered injury, harm, and damages as a result of HSS's unlawful and wrongful conduct. Absent a class action, HSS will continue to maintain Class Members' Personal Information that could be subject to future breaches due to lax or non-existent cybersecurity measures, and such unlawful and improper conduct should not go unchecked nor remedied.

73. Absent a class action, the members of the Class will not be able to effectively litigate these claims and will suffer further harm and losses, as HSS will be allowed to continue such conduct with impunity and benefit from its unlawful conduct.

CLAIMS FOR RELIEF

COUNT I
Negligence
On behalf of Plaintiff and the Class

74. Plaintiff realleges paragraphs 1 through 73 above as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

75. Plaintiff and the Class entrusted their Personal Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Personal Information for business purposes only, and/or not disclose their Personal Information to unauthorized third parties.

76. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the Personal Information were wrongfully disclosed.

77. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Personal Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class.

78. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, configuring, maintaining, and testing Defendant's security protocols to ensure that the Personal Information of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

79. Defendant also had a duty to exercise appropriate clearinghouse practices to remove job applicants' or employees' Personal Information it was no longer required to retain pursuant to regulations.

80. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Personal Information of Plaintiff and the Class.

81. Defendant's duty to use reasonable security measures arose as a result of the relationship that existed between Defendant and Plaintiff and the Class. That relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of applying for jobs with Defendant.

82. Defendant was subject to an independent duty, untethered to any contract between Defendant and Plaintiff or the Class.

83. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

84. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Personal Information of Plaintiff and the Class, the critical importance of providing adequate security of that Personal Information, and the necessity for encrypting it.

85. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to properly configure its network, which held Plaintiff's and Class Members'

sensitive Personal Information, to disallow public access. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the Personal Information of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

86. Plaintiff and the Class had no ability to protect their Personal Information that was in, and possibly remains in, Defendant's possession.

87. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

88. Defendant had and continues to have a duty to adequately disclose that the Personal Information of Plaintiff and the Class within Defendant's possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Personal Information by third parties.

89. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Personal Information of Plaintiff and the Class.

90. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Personal Information of

Plaintiff and the Class during the time the Personal Information was within Defendant's possession or control.

91. Defendant improperly and inadequately safeguarded the Personal Information of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

92. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Personal Information of Plaintiff and the Nationwide Class in the face of increased risk of theft.

93. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Personal Information.

94. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Personal Information it was no longer required to retain pursuant to regulations.

95. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiff and the Class the existence and scope of the Data Breach.

96. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Personal Information of Plaintiff and the Class would not have been compromised.

97. There is a close causal connection between Defendant's failure to implement security measures to protect the Personal Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Personal Information of Plaintiff and the Nationwide Class was stolen as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Personal Information.

98. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

99. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it collected and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

100. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

101. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

102. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class.

103. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate

measures to protect the PII of Plaintiff and the Nationwide Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

104. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

105. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information in its continued possession.

106. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class are entitled to recover actual, consequential, and nominal had a duty to exercise reasonable care and protect and secure Plaintiff's and Class Members' Personal Information. This duty exists at common law and is also codified under Federal law (*see*, *e.g.*, FTCA).

COUNT II
Breach of Implied Contract In Fact
On behalf of Plaintiff and the Class

107. Plaintiff realleges paragraphs 1 through 73 above as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

108. HSS required Plaintiff and the Class to provide their personal information, including names and Social Security numbers, as a condition of applying for employment.

109. As a condition of applying for employment with Defendant, Plaintiff and the Class provided their personal information. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

110. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

111. Defendant breached the implied contracts it made with Plaintiff and the Class by (i) failing to implement technical, administrative, and physical security measures to protect the Personal Information from unauthorized access or disclosure (such as encryption of Social Security numbers) despite such measures being readily available, (ii) failing to limit access to the Personal Information to Defendant's

employees who needed such information to perform a specific job, (iii) failing to store the Personal Information only on servers kept in a secure, restricted access area, and (iv) otherwise failing to safeguard the Personal Information.

112. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

113. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Invasion of Privacy (Electronic Intrusion)
On behalf of Plaintiff and the Class

114. Plaintiff realleges paragraphs 1 through 73 as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

115. Plaintiff and Class Members maintain a privacy interest in their Personal Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above. Plaintiff's and Class Members' Personal Information was contained, stored, and managed electronically in HSS's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities, unique identification numbers, and financial records that were only shared with HSS for the limited purpose of obtaining employment. Additionally, Plaintiff's and Class Members' Personal Information, when contained in electronic form, is highly attractive to criminals who can nefariously use their Personal Information for fraud, identity theft, and other crimes without their knowledge and consent.

116. HSS's disclosure of Plaintiff's and Class Members' Personal Information to unauthorized third-parties as a result of its failure to adequately secure and safeguard their Personal Information is offensive to a reasonable person. HSS's disclosure of Plaintiff's and Class Members' Personal Information to unauthorized third-parties permitted the physical and electronic intrusion into Plaintiff's and Class Members' private quarters where their Personal Information was stored and disclosed private facts about their lives into the public domain.

117. Plaintiff and Class Members have been damaged by HSS's conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT IV
Breach of Confidence
On behalf of Plaintiff and the Class

118. Plaintiff realleges paragraphs 1 through 73 above as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

119. At all times during Plaintiff's and Class Members' relationship with HSS, HSS was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Personal Information.

120. As alleged herein and above, HSS's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' Personal Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

121. Plaintiff and Class Members provided their Personal Information to HSS with the explicit and implicit understandings that HSS would protect and not permit Personal Information to be disseminated to any unauthorized parties.

122. Plaintiff and Class Members also provided their Personal Information to HSS with the explicit and implicit understandings that HSS would take precautions to protect such Personal Information from unauthorized disclosure.

123. HSS voluntarily received in confidence Plaintiff's and Class Members' Personal Information with the understanding that the Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

124. Due to HSS's failure to prevent, detect, or avoid the Data Breach from occurring by, *inter alia*, following industry standard information security practices to secure Plaintiff's and Class Members' Personal Information, Plaintiff's and Class Members' Personal Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

125. As a direct and proximate cause of HSS's actions and/or omissions, Plaintiff and Class Members have suffered damages.

126. But for HSS's disclosure of Plaintiff's and Class Members' Personal Information in violation of the parties' understanding of confidence, their protected Personal Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. HSS's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' protected Personal Information, as well as the resulting damages.

127. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of HSS's unauthorized disclosure of Plaintiff's and Class Members' Personal Information.

128. As a direct and proximate result of HSS's breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from medical fraud, financial fraud, and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Personal Information, which remain in HSS's possession and is subject to further unauthorized disclosures so long as HSS fails to undertake appropriate and adequate measures to protect the Personal Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

129. As a direct and proximate result of HSS's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

130. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 73.

131. Defendant benefited from receiving Plaintiff's and Class Members' Personal Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

132. Defendant also understood and appreciated that Plaintiff's and Class Members' Personal Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

133. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of providing an ability to find people to employ, and in connection thereto, by providing their Personal Information to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their Personal Information. In exchange, Plaintiff and Class Members should have received adequate protection and data security for such Personal Information held by Defendant.

134. Defendant knew Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

135. Defendant failed to provide reasonable security, safeguards, and protections to the Personal Information of Plaintiff and Class Members.

136. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

137. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

138. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

139. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on her own and behalf of all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action pursuant to Federal Rule of Civil Procedure 23, appointing Plaintiff as Class Representative, and the undersigned as Class Counsel;

B. Awarding monetary and actual damages and/or restitution, as appropriate, or nominal damages in the alternative;

C. Awarding declaratory and injunctive relief as permitted by law or equity to assure that the Class has an effective remedy, including enjoining HSS from continuing the unlawful practices as set forth above;

D. Awarding pre- and post-judgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action pursuant to O.C.G.A Section 13-6-11 and as otherwise allowed by law; and

F. Such other and further relief as the Court may deem just and proper.

DATED: August 8, 2023

Respectfully Submitted,

s/ MaryBeth V. Gibson
MaryBeth V. Gibson
Georgia Bar No. 725843
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Telephone: (404) 320-9979
Fax: (404) 320-9978
mgibson@thefinleyfirm.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
Jean S. Martin, Esq.*
Jeanmartin@ForThePeople.com
Francesca K. Burne, Esq. *
Fburne@ForThePeople.com
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 222-4702

Attorneys for Plaintiff and the Putative Class

* (*pro hac vice forthcoming*)